Desempeño de la calidad del servicio (QoS) sobre IPv6

Performance of the quality of service (QoS) over IPv6

Octavio José Salcedo Parra
Ingeniero de Sistemas, Magíster en Teleinformática, Magíster en Economía. Docente de la Universidad Distrital Francisco José de Caldas. Bogotá, Colombia.
ojsalcedop@udistrital.edu.co

Danilo López
Ingeniero Electrónico, Magíster en Teleinformática. Docente de la Universidad Distrital Francisco José de Caldas. Bogotá, Colombia. dalopezs@udistrital.edu.co

Ángela Patricia Ríos
Ingeniera de Sistemas, Magíster en Ciencias de la Información y de las Comunicaciones. Ingenieria Junior de ETB. Bogotá, Colombia. aprios@gmail.com

Clasificación del artículo: investigación (Conciencias)

Fecha de recepción: agosto 21 de 2010 Fecha de aceptación: febrero 1 de 2011

Palabras clave: DivServ, IntSer, IPv6, QoS.

Key words: DivServ, IntSer, IPv6, QoS.

Resumen

Las nuevas aplicaciones como VoIP, e-commerce y videoconferencia son sensibles al desempeño de la red y hacen que la capacidad de las redes de proporcionar Calidad de Servicio sea cada vez más importante. IPv6 se fue desarrollado para resolver algunos de los problemas de IPv4, tales como la QoS, la seguridad y el agotamiento de las direcciones IP. Las redes IP actuales proporcionan un envío de tráfico de mejor esfuerzo, por lo tanto, no ofrecen ningún tipo de garantías de Calidad de Servicio. Sin embargo, existen servicios, entre ellos la voz, con rigurosos requisitos de retardo y variación del retardo (*jitter*), lo que hace necesario añadir funcionalidad a las IP para que las redes basadas en este protocolo sean capaces de soportar este tipo de servicios. Por su parte, IPv6 utiliza dos campos que pueden ser utilizados para implementar QoS: Etiqueta de Flujo y Clase de Tráfico.

En este artículo se describen los mecanismos y las arquitecturas que se utilizan para proporcionar Calidad de Servicio en una red. Posteriormente, se especifican las características que utilizan los protocolos IPv4 e IPv6 para implementar QoS. En las últimas secciones, se presentan los resultados de la comparación de dos escenarios, en los cuales se evalúan.

Abstract
New applications such as VoIP, e-commerce and video conferencing are sensitive to network performance, making the network capacity to provide quality of service is increasingly important. IPv6 was developed to solve some of the problems of IPv4, such as QoS, security and IP address exhaustion. Current IP networks provide better traffic delivery effort, therefore, offer no guarantee of quality service. However, there are services, including voice, with stringent requirements for delay and delay variation (jitter), which makes it necessary to add functionality to IP networks based on this protocol are capable of supporting such services. For its part, IPv6 uses 2 fields that can be used to implement QoS, which are: Flow Label and Traffic Class. This article describes the mechanisms and architectures that are used to provide QoS on a network. Later, you specify the features that use both IPv4 and IPv6 to implement QoS. In the last sections present the results of the comparison of 2 scenarios, which are evaluated

* * *

1. Introducción

Un aspecto clave tanto para usuarios como para los operadores de redes de comunicaciones es garantizar la calidad de servicio (QoS) prestado en las redes de datos y servicios asociados. Para ello, es necesario realizar medidas que permitan comprobar que las redes están proporcionando el servicio contratado. Con el fin de caracterizar la calidad de servicio, numerosas iniciativas como IP Performance Metrics (IPPM) e IP FlowInformationExport (IPFIX) definen métricas y arquitecturas que permiten a todas la partes implicadas llegar a un acuerdo sobre el nivel de calidad de servicio proporcionado y medir su cumplimiento.

Actualmente se dispone de diferentes técnicas para estandarizar y lograr los requerimientos de QoS de las aplicaciones en tiempo real, tales como IntServ, DiffServ y MPLS; las cuales han sido estudiadas para determinar sus ventajas y desventajas [1].

Por su parte, el protocolo IPv4 cuenta con el campo Tipo de Servicio (ToS) para que los paquetes con diferentes opciones de ToS se puedan manejar con diversos niveles de servicio dentro de la red. Debido a que no ha sido clara la definición de este campo, se ha dificultado la construcción de mecanismos de control consistentes y su estandarización, lo que ha conducido a que el ToS no sea ampliamente utilizado [2].

Algunos de los problemas asociados con la QoS en IPv4 son: IPv4 proporciona un modelo fijo y limitado para la diferenciación del tráfico, el campo de prioridades sólo permite codificar prioridades relativas; el campo Tipo de Servicio es demasiado pequeño y no ha sido adoptado, la fragmentación produce congestión y consume muchos recursos de la red, y el protocolo ICMP tiene demasiadas opciones y produce una sobrecarga en los mecanismos de control [3]. Debido a estas limitaciones, Internet Engineering Task Force (IETF) desarrolló una nueva versión del protocolo IP, conocido como IPv6 [4] [5].

2. Calidad de servicio

La calidad del servicio (QoS) se define como la capacidad de una red para proporcionar diversos niveles de servicio a los diferentes tipos de tráfico. Al contar con QoS es posible asegurar una correcta entrega de la información, dando preferencia a aplicaciones de desempeño crítico, donde se comparten simultáneamente los recursos de red con otras aplicaciones no críticas. QoS hace la diferencia al proveer un uso eficiente de los recursos en caso de presentarse congestión en la red, seleccionando un tráfico específico de ésta, priorizándolo según su importancia relativa, y utilizando métodos de control y evasión de la congestión para darles un tra-

tamiento preferencial. Implementando QoS en una red, se logra un rendimiento de ésta más predecible y una utilización de ancho de banda más eficiente.

2.1. Niveles de QoS

Existen tres niveles de servicio: mejor esfuerzo, servicio diferenciado y servicio garantizado.

*a) Mejor esfuerzo o best-effort:*es cuando la red hace todo lo posible para entregar el paquete a su destino, pero no hay garantía de que esto ocurra. Este es el modelo utilizado por las aplicaciones de FTP y HTTP.

b) Servicios integrados: el modelo de Servicios Integrados provee a las aplicaciones de un nivel garantizado de servicio, negociando parámetros de red de extremo a extremo. La aplicación solicita el nivel de servicio necesario con el fin de operar apropiadamente y se basa en la QoS para que se reserven los recursos de red necesarios antes de que la aplicación comience a operar.

c) Servicios diferenciados: este incluye un conjunto de herramientas de clasificación y de mecanismos de cola que proveen a ciertas aplicaciones o protocolos con determinadas prioridades sobre el resto del tráfico en la red.

2.2. Administración de la congestión

La administración de la congestión es un término que abarca diferentes tipos de estrategias de encolamiento para manejar situaciones donde la demanda de ancho de banda de las aplicaciones excede el ancho de banda total que puede proporcionar la red.

2.2.1. FIFO

Es el tipo más simple de encolamiento, consiste en un búfer sencillo que retiene los paquetes salientes hasta que la interfaz de transmisión pueda enviarlos. Los paquetes se envían fuera de la interfaz en el mismo orden en el que llegaron al búfer.

2.2.2. Cola de Prioridad (PQ)

Es un sencillo enfoque para ofrecer un tratamiento preferencial a los paquetes identificados. Los paquetes que llegan a la interfaz se separan en cuatro colas: baja, normal, media y alta prioridad. La salida de estas cuatro colas alimenta un búfer de transmisión de la interfaz. Los paquetes siempre se sirven desde las primeras colas de alta prioridad; este mecanismo se ajusta a condiciones donde existe un tráfico importante, pero puede causar la total falta de atención de colas de menor prioridad.

2.2.3. Cola personalizada (CQ)

Permite al administrador priorizar el tráfico sin los efectos laterales de inanición de las colas de baja prioridad, especificando el número de paquetes o bytes que deben ser atendidos para cada cola. Se pueden crear hasta 16 colas para categorizar el tráfico, donde cada cola es atendida al estilo Round-Robin. CQ ofrece un mecanismo más refinado de encolamiento, pero no asegura una prioridad absoluta como PQ. CQ se utiliza para proveer a tráficos particulares de un ancho de banda garantizado en un punto de posible congestión, asegurando una porción fija del ancho de banda y permitiendo al resto del tráfico utilizar los recursos disponibles.

2.2.4. Weighted Fair Queuing (WFQ)

Este mecanismo asigna una ponderación a cada flujo de forma que determina el orden de tránsito en la cola de paquetes. La ponderación se realiza mediante discriminadores disponibles en TCP/IP (dirección de origen y destino, y tipo de protocolo en IP, número de Socket —puerto de TCP/UDP—) y por el ToS en el protocolo IP. WFQ crea una cola

separada para cada tipo de tráfico y utiliza un valor predeterminado para la profundidad de la cola.

2.2.5. ModifiedDeficit Round Robin (MDRR)

Cuando se configura MDDR para encolamiento, las colas que no están vacías se atienden una tras otra en forma *round robin*. Cada vez que una cola es atendida, una cantidad de datos fija es desencolada y entonces el algoritmo atiende la siguiente cola. Cuando una cola es atendida, MDDR hace seguimiento del número de bytes de datos que fueron desencolados por encima del valor configurado. En el siguiente paso, cuando la cola es atendida nuevamente, menos datos son desencolados para compensar el número de más que fue atendido en el turno anterior. Como resultado, la cantidad promedio de datos atendidos, por cola, será muy cercano al valor configurado. Adicionalmente, MDDR mantiene una cola prioritaria que se atiende de manera preferencial [6].

2.3. Técnicas para evitar la congestión

Los mecanismos descritos no solucionan el problema de congestión; éstos establecen reglas para que el tráfico más sensible tenga cierta prioridad sobre el resto de tráfico. Por otra parte, las técnicas para evitar congestión monitorean el flujo de tráfico de la red con el propósito de anticipar y minimizar su efecto.

2.3.1. Random Early Detection (RED)

Monitorea el tamaño de la cola y cuando ésta alcanza un umbral determinado, selecciona aleatoriamente flujos TCP individuales de los cuales descarta paquetes con el objetivo de indicar al emisor que debe disminuir la tasa de envío.

2.3.2. Weighted Random Early Detection (WRED)

Combina las capacidades del algoritmo RED con la precedencia IP.

2.4. Policing y Modelamiento de Tráfico (TrafficShaping)

Muchas veces es necesario limitar el tráfico saliente en una interfaz determinada, con el fin de administrar eficientemente los recursos de la red. Ante esta necesidad existen dos metodologías de limitación de ancho de banda: Policing y Modelamiento de Tráfico (TrafficShaping). Mediante Policing se especifica la limitación a un máximo de tasa de transmisión para una Clase de Tráfico; si este umbral es excedido, una de las acciones inmediatas será ejecutada: transmitir, descartar, o remarcar. En otras palabras, no es posible almacenar los paquetes para posteriormente enviarlos, como es el caso de TrafficShaping.

Por otra parte, las técnicas deTrafficShaping son un poco más diplomáticas por la manera como operan. En vez de descartar el tráfico que excede cierta tasa determinada, atrasan parte del tráfico sobrante a través de colas, con el fin de modelarla a una tasa que la interfaz remota pueda manejar. El resto del tráfico excedente es inevitablemente descartado.

TrafficShaping (TS) es una buena herramienta en situaciones en las que el tráfico saliente debe respetar una cierta tasa máxima de transmisión. Este proceso es realizado independientemente de la velocidad real del circuito; esto significa que es posible modelar tráficos de Web o FTP a velocidades inferiores a las del receptor. TS puede hacer uso de las listas de acceso para clasificar el flujo y puede aplicar políticas restrictivas de TS a cada flujo. Policing descarta o remarca los paquetes en exceso si es que sobrepasan el límite definido; de esta manera, el tráfico que es originado en ráfagas se propaga por la red, no es suavizado como en TS, y controla la tasa de salida mediante descarte de paquetes, por lo que disminuye el retardo por encolamiento. Sin

embargo, debido a estos descartes, el tamaño de la ventana deslizante de TCP debe reducirse, afectando así el rendimiento global del flujo [7].

2.5. Clasificación y marcado

La clasificación se utiliza para separar paquetes basados en ciertas características, tales como la dirección origen y destino, predefiniendo patrones en el campo ToS de 8 bits del encabezado IP (Precedencia IP o DSCP—DifferentiatedServicesCodePoint—), así como también pueden estar basados en información de protocolos de nivel superior. El campo ToS del encabezado del paquete puede ser reemplazado por los enrutadores con un valor relevante alas políticas de QoS definidas en la red. Esta acción sobre un paquete se denomina marcado [8].

3. Arquitecturas de QoS

Hay 2 arquitecturas de QoS que han sido propuestas y estandarizadas por la IETF. La primera se denomina Servicios Integrados (IntServ) y la segunda, Servicios Diferenciados (DiffServ). IntServ provee QoS a través de la reserva de recursos a lo largo del camino de datos, antes de iniciar la transmisión de los paquetes. Por otra parte, DiffServ incluye un conjunto de herramientas de clasificación y de mecanismos de cola que proveen a ciertas aplicaciones o protocolos, determinadas prioridades sobre el resto del tráfico en la red.

3.1. Servicios Integrados

La primera arquitectura propuesta para ofrecer QoS en IP fue la arquitectura de Servicios Integrados o IntServRFC 1633 [9]. Ésta se basa en garantizar QoS a través de la reserva de recursos extremo a extremo para cada flujo.

El modelo se sustenta en los siguientes supuestos:

- Los recursos se deben gestionar de forma directa y explícita para satisfacer los requerimientos de las aplicaciones. Esto implica la utilización de mecanismos para control de admisión y reservación de recursos.

- Internet debe ser la infraestructura común para el tráfico normal y el de tiempo real, ya que construir una nueva red para el tráfico de tiempo real sería demasiado complejo. Esto implica que se debe unificar la pila de protocolos para cualquier tipo de tráfico, es decir, IP debe ser utilizado también para el transporte de datos de tiempo real.

Cada flujo se debe atender independientemente y no puede influenciar a otros. La arquitectura define dos clases de servicio adicionales al mejor esfuerzo: servicio garantizado y servicio de carga controlada, las cuales especifican el tratamiento que deben recibir los flujos a lo largo del camino. Además, IntServ requiere que los recursos necesarios para satisfacer los requerimientos de una aplicación o servicio se reserven sobre el trayecto con anticipación, para lo cual es necesario el Protocolo de Reservación de Recursos (RSVP). Éste utiliza un conjunto de mensajes de señalización para transportar información sobre los requerimientos y propiedades de cada flujo, la cual se utiliza para mantener tablas de estado en cada uno de los nodos, generando así un alto tráfico de señalización y ocupación de recursos en los dispositivos [10].

3.2. Servicios diferenciados

DiffServ se basa en la división del tráfico en un número limitado de clases de servicio, trasladando el procesamiento más complejo a los nodos de frontera del dominio. DiffServ no necesita que una aplicación reserve recursos para cada flujo sino que los requerimientos de QoS de los usuarios se especifiquen en un Acuerdo de Nivel de Servicio (SLA) [11].

Todo el tráfico que ingresa a un dominio DiffServ se clasifica asignándosele un comportamiento de reenvío predeterminado denominado Comportamiento por Saltos (PHB) (Per Hop Behavior). Es por esto que los paquetes deben marcarse con un código que diferencia los distintos comportamientos. La marca se realiza cambiando un campo del encabezado IP, particularmente el tipo de servicio por un código denominado DSCP que consta de seis bits para diferenciar clases de tráfico y dos bits reservados [12]. El código se asigna en los terminales o en el enrutador de ingreso al dominio DiffServ y se examina en cada uno de los nodos del trayecto con el fin de gestionar colas y controlar los mecanismos de planificación en los enrutadores.

Se han definido dos PHBs adicionales al mejor esfuerzo que conforman las nuevas clases de servicio que se describen a continuación. El Reenvío Expedito (EF) proporciona un servicio de baja pérdida de paquetes, bajo retardo, bajo *jitter* y ancho de banda asegurado que es equivalente al servicio llamado Línea Arrendada Virtual. Los paquetes pertenecientes al PHBEF se marcan con el código 101110. Por otra parte, el Reenvío Asegurado (AF) proporciona una alta probabilidad de que los parámetros del tráfico sean conformes a los acuerdos; aunque se permite que el cliente genere más tráfico del acordado, el exceso no será tratado de la misma manera; además, se definen cuatro clases de AF con diferentes niveles de prioridad y con marcas que permiten saber qué paquetes se eliminarán primero en caso de congestión.

Es importante señalar que dado a que la marcación de tráfico se realiza en el ingreso al dominio DiffServ, la calidad de servicio se garantiza únicamente en una dirección.

4. QoS en IPv6

El campo ToS fue implementado dentro del grupo de diseño de IPv4 como un campo de ocho bits, compuesto por un valor de precedencia IP de tres bits y cuatro bits indicadores. Su función es especificar parámetros de prioridad, retardo, rendimiento y fiabilidad. De este modo, los paquetes con diversas opciones de ToS se pueden manejar con diferentes niveles de servicio dentro de la red.

De acuerdo a la recomendación RFC 791 [13], el ToS proporciona una indicación de los parámetros de calidad de servicio deseados. Éstos se utilizan para especificar el tratamiento del datagrama durante su transmisión en una red en particular. Algunas redes ofrecen prioridad de servicio, lo cual consiste en considerar el tráfico de alta prioridad como más importante que el resto (generalmente aceptando sólo tráfico por encima de cierta prioridad en momentos de sobrecarga). La elección más común es un compromiso de tres factores: bajo retardo, alta fiabilidad y alto rendimiento.

El campo ToS está compuesto por un campo de precedencia, tres indicadores D, T, R y dos bits no utilizados; el campo de precedencia utiliza ocho niveles, de cero (rutinaria) a siete (paquete de control de red); los tres bits indicadores permiten especificar qué es lo que más interesa, el retardo, el rendimiento o la fiabilidad. A continuación se presenta un resumen del campo ToS:

- Bits 0-2 : prioridad.
- Bit 3:0 = retardo normal, 1 = bajo retardo.
- Bit 4:0 = rendimiento normal, 1 = alto rendimiento.
- Bit 5: 0 = fiabilidad normal, 1 = alta fiabilidad.
- Bits 6-7: reservado para uso futuro.

El subcampo de precedencia es una medida de importancia relativa al datagrama. Se utilizan ocho-niveles de precedencia. IP tratará de proporcionar un tratamiento preferencial a los diagramas con precedencias superiores.

- 111 - Control de Red
- 110 - Control Entre Redes
- 101 - CRITICO/ECP
- 100 - Muy urgente (Flash Override)
- 011 - Urgente (Flash)
- 010 - Inmediato
- 001 - Prioridad
- 000 - Rutina

El uso de los indicadores de retardo, rendimiento y fiabilidad puede incrementar el coste (en cierto sentido) del servicio. En muchas redes un mejor desempeño de uno de estos parámetros significa un peor desempeño de otro. Por lo tanto, excepto para casos excepcionales, no se deben establecer más de dos indicadores.

Por su parte, el protocolo IPv6 tiene dos campos que pueden ser utilizados como herramientas para implementar QoS: Etiqueta de Flujo y Clase de Tráfico [5].

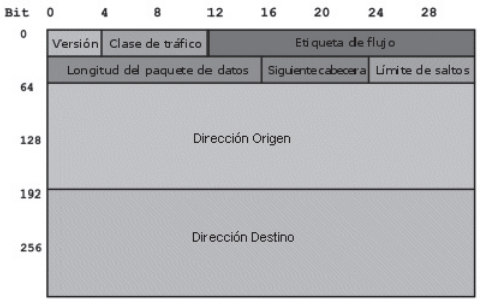

Figura 1. Estructura del encabezado de un paquete IPv6.

El campo Etiqueta de Flujo de 20 bits en la cabecera IPv6 se agrega para permitir el etiquetado de paquetes que pertenecen a flujos de tráfico particulares y puede ser usado por el origen para etiquetar secuencias de paquetes para las cuales solicita un manejo especial por parte de los enrutadores IPv6, tal como la calidad de servicio no estándar o el servicio en tiempo real. Se exige a los *hosts* o a los enrutadores, que no dan soporte a las funciones del campo Etiqueta de Flujo, poner el campo en cero al enviar un paquete, pasar el campo inalterado al reenviar un paquete e ignorar el campo al recibir un paquete.

El campo de ocho bits Clase de Tráfico en la cabecera IPv6 es utilizado por los nodos origen y/o enrutadores intermedios para identificar y distinguir entre las diferentes clases o prioridades de paquetes IPv6; su función es similar al campo ToS de IPv4.

Los siguientes requisitos generales se aplican al campo Clase de Tráfico:

- La interface de servicio para el servicio IPv6 dentro de un nodo debe proporcionar un medio para que un protocolo de capa superior proporcione el valor de los bits Clase de Tráfico en los paquetes originados por éste. El valor por defecto debe ser cero para todos los ocho bits.

- Los nodos que soportan un uso específico de algunos o todos los bits Clase de Tráfico se les permite cambiarlos en los paquetes que los nodos originan, reenvían o reciben, como sea requerido para ese uso específico. Los nodos deben ignorar y dejar sin alterar los bits del campo Clase de Tráfico para los cuales no dan soporte a un uso específico.

- Un protocolo de capa superior no debe asumir que el valor de los bits Clase de Tráfico en un paquete recibido es el mismo que el valor enviado por el origen del paquete.

5. Simulación y resultados

5.1. Simulación

Se utiliza la herramienta Opnet para simular dos escenarios en los cuales se evalúa la QoS de la red, la cual está compuesta por dos sedes de una empresa, conectadas a través de un enlace de 1Mbps y que requieren utilizar un aplicativo de videoconferencia; también se utiliza una política de tráfico en la interfaz saliente del enrutador de Medellín para manejar la asignación de ancho de banda; se emplean listas de control de acceso para clasificar los flujos de tráfico en clases de tráfico de acuerdo a la dirección origen y a cada flujo se le asigna un porcentaje del ancho de banda.

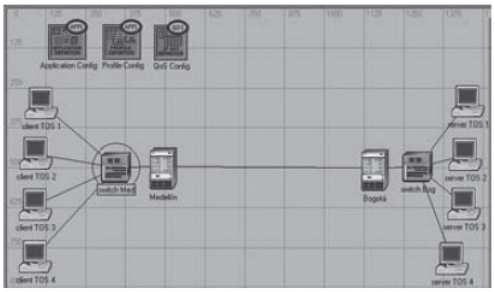

Figura 2. Topología de red.

La diferenciación de los distintos flujos se hace mediante el campo ToS proporcionado por los datagramas IP. Un ToS diferente puede ser seleccionado para cada flujo de tráfico definido en la red. Una vez caracterizado en una de las categorías IP-ToS, el tráfico es etiquetado con el ToS especificado y experimenta un servicio diferenciado en la red. A través de esta diferenciación, el tráfico sufre un encolamiento que depende del tráfico existente en otras colas en las que está compitiendo por el mismo interfaz de salida. Para este caso, se utiliza MDRR como mecanismo de encolamiento y cuatro pares de clientes de videoconferencia, cada par usa diferente ToS.

5.2. Resultados

En las siguientes gráficas se muestran los resultados comparando el retardo y el tráfico enviado y recibido en cada uno de los dos modelos teniendo en cuenta la prioridad.

En las Figuras 3 y 4 se observa el retardo extremo a extremo para los clientes con menor y mayor prioridad; el cliente con mayor prioridad tiene un retardo menor.

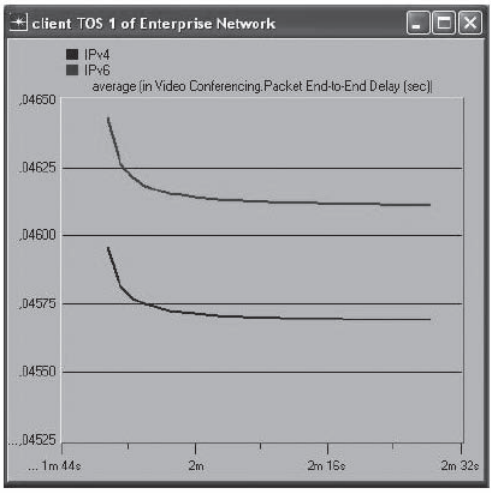

Figura 3. Retardo global para el cliente con baja prioridad.

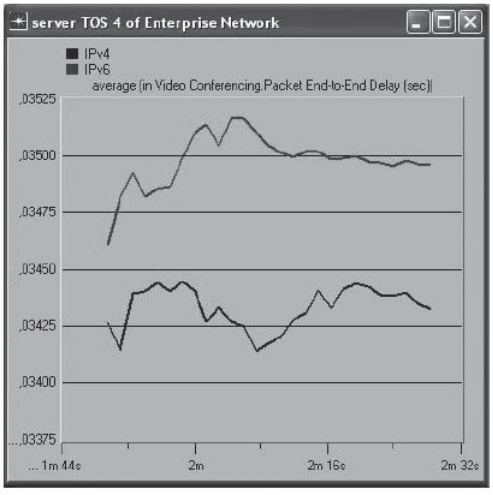

Figura 4. Retardo global para el cliente con alta prioridad.

Al utilizar como mecanismo de clasificación el campo ToS del paquete IPv4 y el campo Clase de Tráfico IPv6, se obtienen resultados similares y es posible emplear las mismas técnicas y arquitecturas que se utilizaban en IPv4.

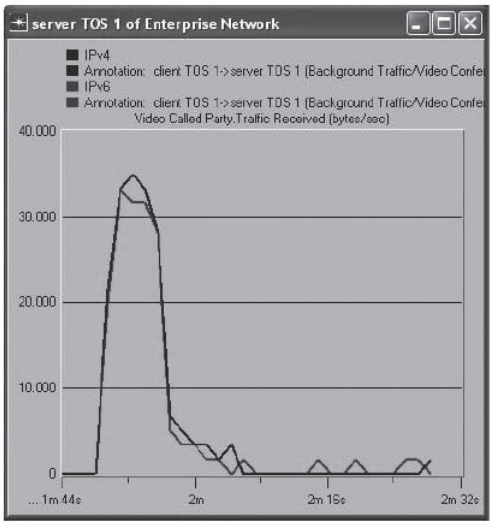

Figura 5. Tráfico recibido para el cliente con baja prioridad.

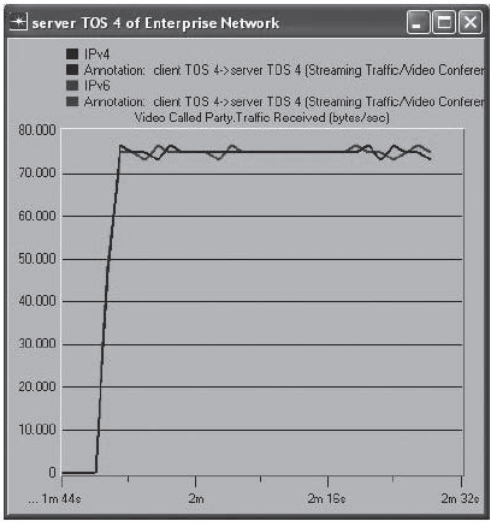

Figura 6. Tráfico recibido para el cliente con alta prioridad.

6. Conclusiones

Tanto los mecanismos como las arquitecturas utilizadas para proveer Calidad de Servicio en una red son implementados de la misma forma en ambas versiones de IP. La diferencia entre la QoS de IPv4 e IPv6 se centra en el proceso de clasificación del tráfico en el que los paquetes o flujos son diferenciados a través de varios parámetros tales como la dirección de origen o destino, DSCP o los valores de precedencia IP y los tipos de protocolos de nivel superior. IPv6 proporciona mayor facilidad de clasificar los paquetes con identificadores de tráfico. Adicionalmente, el campo Etiqueta de Flujo tiene la ventaja de estar localizado antes de los campos de dirección, lo que ayuda a reducir los retardos en la verificación del paquete.

Referencias bibliográficas

[1] Internet Protocol versión 6. RFC 2460. Diciembre 1998.

[2] *An Architecture for Differentiated Services*. RFC 2475. Diciembre 1998.

[3] C.Popoviciu, E. Levy-Abegnoli, P. Grossetete,"Deploying IPv6 Networks". *Cisco Press*, p. 176, 2006

[4] S. Álvarez, A. González, *Estudio y Configuración de Calidad de Servicio para Protocolos IPv4 e IPv6 en una Red de Fibra Óptica WDM*, [en línea]. Disponible en: http://www.elo.utfsm.cl/investigacion/publicaciones/2005/QoS_RevIngUTA.pdf

[5] *ResourceReservationProtocol* . RFC 2208. Septiembre 1997.

[6] A. López, *Calidad de Servicio en IPv6*, [en línea]. Disponible en: http://www.redes-linux.com/manuales/ipv6/alberto_lopez_QoS tutorial.pdf

[7] M. Flannagan,"Administering Cisco QoS for IP Networks",*Sungress,* 2001.

[8] *Integrated Services in the Internet Architecture: an Overview*. RFC 1633. Junio 1994.

[9] E. Fgee, J.D. Kenney, W.J. Phillips, W. Robertson, S. Sivakumar, "Comparison of QoS performance between IPv6 QoS management model and IntServ and DiffServQoS models",*Communication Networks and Services Research Conference*, Proceedings of the 3rd Annual. 2005, pp. 287- 292. 2005

[10] M. Flannagan, "Administering Cisco QoS for IP Networks (Paperback)", *Syngress*, 2001.

[11] IP Version 6 Working Group (IPv6), [en línea]. Disponible en: http://www.ietf.org/html.charters/ipv6-charter.html

[12] *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*. RFC 2474. Diciembre 1998.

[13] Internet Protocol DARPA Internet, ProgramProtocolSpecification. RFC 791. Septiembre 1981.